First concepts

Terminology

What is Security?

• Definitions from the Amer. Herit. Dict.:
  – Freedom from risk or danger; safety. (NO!)
  – Measures adopted … to prevent a crime such as burglary or assault. (ALMOST!)

• Network security measures:
  – Mechanisms to prevent, detect, and recover from network attacks, or for auditing purposes.
Terminology

• Assets and liabilities
• Policies
• Security breeches
• Vulnerabilities
• Attacks
• Threats
• Threat Intensity

A Secured Network

• A network is “secured” if it has deployed adequate measures for prevention of, detection of, and recovery from attacks.
  – Adequate = commensurate with the value of the network’s assets and liabilities, and the perceived threat intensity.
  – By Breno
Security Goals

- Confidentiality
- Integrity
- Availability

Other important security goals include auditability

Security operations

- **Prevention** against adversarial or accidental capture and/or modification of information.
- **Audit** of data accesses/modifications, and of privileged operations.
- **Detection** of all improper access to data and system resources.
- **Recovery** from unauthorized access, restoring data values, system integrity, and identifying compromised data/resources.
- **Retaliation** (legal, PR, info. warfare)
**Authentication**

- Authentication mechanisms comprise a substantial portion of this course.
- Used to prevent impersonation and detect unauthorized data modifications.
- Some mechanisms to provide data integrity will not be considered:
  - Enforcement of safe data manipulation methods (file system protection mechanisms, database protection mechanisms).

**Availability**

- Continuous service, quality of service, resource wastefulness reduction
  - Typical attack: DoS, DDoS
- Prevention by removal of bottlenecks
- **Detection** of attacks
- **Recovery** of service provision ability
- **Audit** of service requests
Concrete Security Measures

• Securing an open network requires adoption of a myriad of measures:
  – Policies, audit and evaluation
  – Personnel training
  – Physical security/ EM emanation shielding
  – Authentication and access control
  – Communication security: Cryptography-based techniques.

Open Systems Interconnection

A standard-centric networking model
Open Systems

- Open Systems:
  - general-purpose networks that support standardized communication protocols and may accommodate heterogeneous sub-networks transparently.
  - Corporate Intranets:
    - Ethernet, Token Ring and Wireless subnets.
  - Internet

Open Systems
Interconnection Model

<table>
<thead>
<tr>
<th>ISO’s layered approach to standardization</th>
<th>7. Application layer</th>
<th>FTP, Telnet, SSH</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Presentation layer</td>
<td>MIME, XDR, SSH</td>
<td></td>
</tr>
<tr>
<td>5. Session layer</td>
<td>NetBIOS, FTP, Telnet, SSH</td>
<td></td>
</tr>
<tr>
<td>4. Transport layer</td>
<td>TCP, UDP, SSL/TLS</td>
<td></td>
</tr>
<tr>
<td>3. Network layer</td>
<td>IP, ICMP, IPSEC</td>
<td></td>
</tr>
<tr>
<td>2. Data link layer</td>
<td>Ethernet, PPP, ISDN</td>
<td></td>
</tr>
<tr>
<td>1. Physical layer</td>
<td>pins, cabling, radio</td>
<td></td>
</tr>
</tbody>
</table>
1-2. Physical/Data Link Layers

- Physical layer: Radio, fiber, cable, pins
- Data link layer orchestrates the signaling capabilities of the physical medium (unreliable, noisy channel) into reliable transmission of protocol data units (PDUs).
- PDUs contain control information, addressing data, and user data.
- Hardware-based encryption operates at 1+2.

3. Network Layer

- Exports a logical network interface, allowing for uniform addressing and routing over heterogeneous subnetworks.
  - E.g.: IP can route between Ethernet- and 802.11x - networks
4. Transport Layer

- Permits connection and connectionless associations. Connections enable reliable transmission of data streams.
- End-to-end security first becomes meaningful at this level.
  - Security associations: An association is either a connection or a connectionless transmission service at levels 4-7.
Levels 5 and Higher

• Application through session protocol layers.
  – Many network applications implement their own session management. Moreover, they typically depend on system libraries for presentation layer capabilities. Such applications, from a data-path viewpoint, may be considered a single layer: PDUs only typically appear at the session layer.

Example: SSH

• SSH provides services at all topmost three OSI layers.
  – Application: Terminal/file transfer
  – Presentation: Encryption
  – Session: Connection, synchronization
• Only at the session layer the data (encrypted buffers of user input) gets first packaged into a protocol data unit for transmission.
TCP/IP networking model

A data-path centric model

TCP/IP network model

(≠ TCP/IP Protocol)

<table>
<thead>
<tr>
<th>TCP/IP Layer</th>
<th>OSI Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP Application Layer</td>
<td>7. OSI Application</td>
</tr>
<tr>
<td>TCP/IP Transport Layer</td>
<td>6. OSI Presentation</td>
</tr>
<tr>
<td>TCP/IP Network Layer</td>
<td>5. OSI Session</td>
</tr>
<tr>
<td>TCP/IP Data Link Layer</td>
<td>4. OSI Transport</td>
</tr>
<tr>
<td>TCP/IP Physical Layer</td>
<td>3. OSI Network</td>
</tr>
<tr>
<td></td>
<td>2. OSI Data Link Layer</td>
</tr>
<tr>
<td></td>
<td>1. OSI Physical Layer</td>
</tr>
</tbody>
</table>
Protocol Data Wrapping

Sending host:
- rlogin host
- TCP segment
- IP datagram/packet
- Data link layer
- Physical layer

Receiving host:
- Application Layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

Transmission medium

Protocol Wrapper Dependencies and Network Layers

Application Layer:
- rlogin
- Telnet
- FTP
- SMTP
- RGP

Transport layer:
- NFS
- TFTP
- ICMP
- TCP
- OSPF

Network layer:
- UDP
- ICMP
- ARP
- RARP

Hardware or link layer:
- Ethernet
- SLIP
- PPP
Fitting Security

How security measures fit into the network models

Association Model

• An association is either a connectionless data transmission service or a connection at any of OSI layers 4-7, or TCP/IP application /transport layers
• An N-association is the data-path through which N+1 entities communicate:
  – Generally at session layer or below.
  – N+1-layer data packaged into N-PDUs
Association Model (2)

Security at levels 1 - 3

- Implemented at the host/network interface level (lack notion of association): Link-to-link security.
- Encryption/authentication requires operations at each network node.
- Each network node must be trusted.
  - Impractical for Open Systems?
Security protocols \( \leq 3 \)

- Many VPN technologies work at level 2
  - PPTP, L2F, L2TP
  - Rationale: Directed at dial-up VPN networks, (PPP is level-2). Provide service to a variety of network-level protocols, such as IP or IPX.

Security above level 3

- Most flexible security measures
- End-to-end security: The security policies and mechanisms can be based on associations between entities (applications, processes, connections), as opposed to host-based:
  - In multi-user environments, or when hosts are not physically secure, host-based policies are not sufficiently fine-grained.
Summary

• Security measures can take three main forms:
  1. End-to-end security at the TCP/IP application layer (5-7 OSI model layers)
  2. End-to-end security at the (TCP/IP, OSI) transport layer
  3. Link-to-link security at the network, data-link and physical layers.

Attacks

A taxonomy
Attack Types

And their impact on end-to-end communication security mechanisms

Passive Attacks

• Observation of N+1-layer data in an N-layer PDU: release of data contents, or eavesdropping
• Observation of control/ address information on the N-PDU itself: traffic analysis.
• Transport/network boundary = End-to-end/ link-to-link boundary.
  — Traffic analysis is least effective if N+1 = 4.
Active Attacks

- Impersonation
- Packet injection (attacker-generated PDU)
- Packet deletion/delay
- Packet modification/re-ordering
- Replay attacks

• If a breech can be achieved by both active and passive attacks, which is more powerful? (problematic)